UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,178	08/14/2001	Donald P. Matthews JR.	2875.0500001	8980

26111 7590 11/04/2008

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
11/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/929,178	MATTHEWS, DONALD P.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,3,28-30,32-36 and 44-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,3,28-30,32-36 and 44-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 June 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20080919*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 2, 3, 28-30, 32-36, and 44-46 are pending.

A complete copy of the SSL reference cited below is provided with this office action to supplement the previous partial copy, such that the newly cited portions can be seen therein.

Response to Arguments

1. Applicant's arguments with respect to claims 2, 3, 28-30, 32-36, and 44-46 have been considered but are moot in view of the new ground(s) of rejection. Regarding the previous 112, first paragraph rejection, the Examiner notes that the referenced portions of the application discuss SSL and TLS being the network security protocol, and as such, the SSL reference described below has been cited to explicitly show the formation of a data block to be [remaining payload, MAC, padding], as appears to be the case in the application. Additionally, the TLS reference could be used equally well to show the formation of such a data block (in particular, feeding of the MAC to an encryption component, appending it to the payload, adding any required padding, then encrypting the remaining payload with the MAC and padding). The new limitation is worded rather ambiguously (it does not make clear that this is the formation, but rather could correspond to adding padding to both the remaining payload and the authentication code), however, the limitation has been construed as providing a data block as the formation just described for clarity, with respect to the SSL reference.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 2, 28-30, 33, 35, 36, and 44-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan (U.S. Patent 6,704,871) in view of Larsen (U.S. Patent 7,068,791), Huynh (U.S. Patent 6,983,366), and SSL3spec (Freier et al., "The SSL Protocol Version 3.0", 11/18/1996, pp. 1-62).

Regarding Claim 46,

Kaplan discloses a method for accelerating cryptographic processing of a plurality of data packets according to a network security protocol, comprising:

Receiving, in a chip, data for a first packet from an off-chip processor (Column 27, line 55 to Column 29, line 12; Column 39, lines 25-42; Column 41, lines 16-51; and Column 43, line 1 to Column 44, line 31);

Performing authentication operations on data for the first packet to generate an authentication code (Column 37, line 41 to Column 38, line 62);

Performing encryption operations on a set of data for the first packet, wherein the encryption operations on the set of data for the first

packet are performed in parallel with the authentication operations for the first packet (Column 37, line 41 to Column 38, line 62);

Receiving, in the chip, data for a second packet (Column 27, line 55 to Column 29, line 12; Column 37, line 41 to Column 38, line 62; Column 39, lines 25-42; Column 41, lines 16-51; and Column 43, line 1 to Column 44, line);

Adding padding to data for the first packet and the authentication code for the first packet to generate a data block having a predefined length (Column 37, line 41 to Column 38, line 62; Column 39, lines 26-42; Column 41, lines 16-51; and Column 42, lines 29-54);

Performing encryption operations on remaining payload data for the first packet, the authentication code for the first packet, and padding (Column 37, line 41 to Column 38, line 62);

Performing authentication operations on data for the second packet (Column 37, line 41 to Column 38, line 62);

Passing the cryptographically processed first packet from the chip to the off-chip processor (Column 27, line 55 to Column 29, line 12; and Column 43, line 1 to Column 44, line 31);

Wherein the authentication and encryption operations for the first packet are performed within the chip in a single pass (Column 37, line 41 to Column 38, line 62; and Column 41, lines 16-51);

But does not explicitly disclose that the authentication operations are performed on a set of header data and the payload data of the packet, that the padding is added so as to form a data block such as [remaining payload, MAC, padding] (this is not in the claim limitation, but it shows the formation that the Examiner believes that Applicant is going for), or that the authentication operations for the second packet are performed simultaneously with the encryption operations on remaining payload data and authentication and authentication code for the first packet.

Larsen, however, discloses that the authentication operations are performed on a set of header data and the payload data of the packets (Column 7, lines 6-45). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure packet system of Larsen into the cryptographic co-processor of Kaplan in order to provide multiple authentication codes within each packet, thereby allowing the system to determine whether a message came from a proper sender via the header's authentication code, so as to allow for adaptive retransmission, even when the payload of the packet was received in error (and thus, the packet's authentication code is incorrect).

Huynh, however, discloses that the authentication operations for the second packet are performed simultaneously with the encryption operations on the remaining data to be encrypted for the first packet (Column 2, lines 24-35; Column 6, lines 19-38; and Column 8, lien 23 to

Column 9, line 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the packet processing techniques of Huynh into the cryptographic co-processor of Kaplan as modified by Larsen in order to allow another packet to be processed as soon as a particular resource (encryption or authentication unit) becomes available, so the system need not wait until the first packet is completely processed before beginning processing of another packet, thereby allowing the system to process network security protocol data faster and more efficiently.

SSL3spec, however, discloses adding padding to remaining payload data for a packet and the authentication code for the packet to generate a data block having a predefined length so as to form a data block such as [remaining payload, MAC, padding]; and performing encryption operations on such a data block (Pages 14-15, Section 5.2.3.2; and Appendix F.2 on page 57). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of SSL3spec into the cryptographic co-processor of Kaplan as modified by Larsen and Huynh in order to gain cryptographic security between two parties and interoperability between differently coded programs (Page 4, Sections 2.1, 2.2, and 2.3).

Regarding Claim 2,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 46, in addition, SSL3spec discloses that the network security protocol is SSLv3 (Pages 3-4, Section 1; and Page 10, Section 5.0).

Regarding Claim 28,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 46, in addition, Kaplan discloses aligning the received set of header data for the first packet (Column 39, lines 25-42; Column 43, lines 1-28; and Column 44, lines 35-43).

Regarding Claim 29,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 28, in addition, Kaplan discloses storing the aligned set of header data for the first packet in a FIFO to accumulate a predefined amount of data before commencing the authentication operations (Column 38, lines 50-57).

Regarding Claim 30,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 29, in addition, Kaplan discloses that the predefined amount of data comprises 512 bits (Column 38, lines 50-57).

Regarding Claim 33,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 46, in addition, Kaplan discloses aligning, for encryption

operations, the set of data in the payload data for the first packet to provide aligned data for the encryption operations (Column 39, lines 26-42).

Regarding Claim 35,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 33, in addition, Kaplan discloses that aligning, for encryption operations, comprises adding padding (Column 39, lines 26-42).

Regarding Claim 36,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 33, in addition, Kaplan discloses storing the aligned set of data in the payload data for the first packet for the encryption operations in a FIFO to accumulate a predefined amount of data before commencing the encryption operations (Column 39, lines 26-42; and Column 40, lines 43-52).

Regarding Claim 44,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 46, in addition, Kaplan discloses that the authentication operations are performed by an authentication component of the chip, the encryption operations are performed by an encryption component of the chip, and authentication data generated by the authentication component is passed to the encryption component and aligned by the encryption

component (Column 38, lines 58-62; Column 39, lines 25-42; Column 40, line 42 to Column 41, line 15; Column 42, lines 12-29; and Figure 9); and SSL3spec discloses passing authentication data to an encryption component (Pages 14-15, Section 5.2.3.2; and Appendix F.2 on page 57).

Regarding Claim 45,

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 46, in addition, Kaplan discloses that the authentication operations are performed by an authentication component of the chip, the encryption operations are performed by an encryption component of the chip, and decrypted data generated by the encryption component is passed to the authentication component and aligned by the authentication component (Column 38, lines 58-62; Column 39, lines 25-42; Column 40, line 42 to Column 41, line 15; Column 42, lines 12-29; and Figure 9).

3. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan in view of Larsen, Huynh, and SSL3spec, further in view of TLSspec (Dierks et al., "The TLS Protocol Version 1.0", 10/28/1997, pp. 1-12).

Kaplan as modified by Larsen, Huynh, and SSL3spec does not explicitly disclose that the network security protocol is TLS.

TLSspec, however, discloses that the network security protocol is TLS (Pages 3-4, Section 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol

of TLSspec into the cryptographic co-processor of Kaplan as modified by Larsen, Huynh, and SSL3spec in order to gain extensibility to other protocols and methods (Pages 4-5, Sections 2.1, 2.2, and 2.3).

4. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan in view of Larsen, Huynh, and SSL3spec, further in view of Ganapathy (U.S, Patent 6,557,096).

Kaplan as modified by Larsen, Huynh, and SSL3spec discloses the method of claim 28, in addition, Larsen discloses that head data for the first packet comprises Content Type and Length (Column 7, lines 6-45; and Column 9, lines 1-23); but does not explicitly disclose that the data is aligned into rows of data where each row of data contains a single type of data.

Ganapathy, however, discloses that the data is aligned into rows of data where each row of data contains a single type of data (Column 17, lines 38-55; Column 19, line 35 to Column 20, line 25; and Figure 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data aligner of Ganapathy into the cryptographic co-processor of Kaplan as modified by Larsen, Huynh, and SSL3spec in order to properly align and format the data before sending it for mathematical (in this case, authentication and encryption/decryption) operations, so that the data has any needed sign and guard bids pre-pended thereto.

5. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan in view of Larsen, Huynh, and SSL3spec, further in view of Gaytan (U.S. Patent 5,638,367).

Kaplan as modified by Larsen, Huynh, and SSL3spec does not explicitly disclose that aligning comprises removing non-valid data.

Gaytan, however, discloses that aligning comprises removing non-valid data (Column 1, line 62 to Column 2, line 29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data packing system of Gaytan into the cryptographic co-processor of Kaplan as modified by Larsen, Huynh, and SSL3spec in order to gain better throughput and performance by only sending valid data past the buffer.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/

Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437